Polynômes cyclotomiques. Théorème de Wedderburn

Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159, France
dany-jack.mercier@univ-ag.fr

27 mars 2003

Dans toute la suite, n désigne un entier strictement positif et K un corps commutatif de caractéristique p éventuellement nulle. Si $p = 0$, alors K est une extension de $\mathbb{Q}$. Si p est un nombre premier, K est une extension du corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1 Définitions

Définition 1 *Le corps de décomposition du polynôme $x^n - 1$ sur K est appelé **n-ième corps cyclotomique sur K**, et noté $\Sigma_n(K)$ ou Σ_n. Les racines du polynôme $x^n - 1$ dans Σ_n sont appelées les **n-ièmes racines de l'unité sur K** et l'ensemble de ces racines est noté $\Gamma_n(K)$ ou Γ_n.*

Si $K = \mathbb{R}$, alors $\Sigma_n(\mathbb{R}) = \mathbb{C}$ et $\Gamma_n(\mathbb{C}) = \left\{ e^{ik\frac{2\pi}{n}} \,/\, 0 \leq k \leq n-1 \right\}$ s'interpréte géométriquement comme l'ensemble des sommets d'un polygone régulier à n côtés.

L'ensemble Γ_n est un sous-groupe multiplicatif de $(\Sigma_n^*, \times)$ puisqu'il contient 1 et que $a, b \in \Gamma_n$ entraîne $ab^{-1} \in \Gamma_n$. Par conséquent Γ_n sera cyclique comme tout sous-groupe fini du groupe multiplicatif d'un corps commutatif.

D'autre part, le polynôme $x^n - 1$ et son polynôme dérivé nx^{n-1} admettent au moins une racine commune si et seulement si p divise n. On en déduit que les racines de $x^n - 1$ sont toutes distinctes si p ne divise pas n. Par contre, si la caractéristique p divise n, et si l'on pose $n = p^s m$ avec $\mathrm{pgcd}(m, p) = 1$, on obtient

$$x^n - 1 = x^{p^s m} - 1 = (x^m - 1)^{p^s}.$$

Cela montre que $\Gamma_n(K) = \Gamma_m(K)$ et que $x^n - 1$ possède m racines distinctes, chacune étant de multiplicité $\frac{n}{m}$. En rappelant qu'un polynôme séparable est un polynôme dont toutes les racines sont simples dans son corps de décomposition, on a montré :

Théorème 1 *1) Si p ne divise pas n, alors Γ_n est un sous-groupe cyclique d'ordre n de $(\Sigma_n^*, \times)$, et $x^n - 1$ est un polynôme séparable.*

[0] [ccof0003] v1.00β http://perso.wanadoo.fr/megamaths

2) Si p divise n et si l'on note $n = p^s m$ avec $\text{pgcd}(m,p) = 1$, alors $\Gamma_n(K) = \Gamma_m(K)$ et $\Sigma_n(K) = \Sigma_m(K)$. Dans ce cas $x^n - 1$ possède m racines distinctes, chacune étant de multiplicité $\frac{n}{m}$.

Pour l'étude de $\Gamma_n(\mathbb{F}_q)$ on pourra donc supposer que $\text{pgcd}(n,p) = 1$.

Définition 2 *Soit n un entier non nul et non divisible par p. Un générateur du groupe $(\Gamma_n, \times)$ est appelé **racine n-ième primitive de l'unité sur** K. Le polynôme unitaire Q_n dont les racines sont les racines primitives n-ièmes de l'unité est appelé **polynôme cyclotomique d'indice** n **sur** $\mathbb{F}_q$.*

Si ξ désigne une racine primitive n-ième de l'unité, alors $\Gamma_n = \left\{1, \xi, ..., \xi^{n-1}\right\}$ et toutes les racines primitive n-ièmes de l'unité sont données par ξ^i avec $\text{pgcd}(i,n) = 1$. On a donc

$$Q_n(x) = \prod_{\text{pgcd}(i,n)=1} \left(x - \xi^i\right).$$

2 Relation fondamentale

On suppose toujours que n est un entier non nul et non divisible par p.

Théorème 2

$$x^n - 1 = \prod_{d|n} Q_d(x).$$

Preuve : Notons toujours $\Gamma_n = \left\{1, \xi, ..., \xi^{n-1}\right\}$ l'ensemble des racines de $x^n - 1$. Pour tout diviseur d de n, notons $\mathcal{R}_d$ l'ensemble des racines d-ièmes primitives de l'unité. On a $\mathcal{R}_d \subset \Gamma_n$, et la famille $\{\mathcal{R}_d\}_{d|n}$ forme une partition de Γ_n. Par suite

$$x^n - 1 = \prod_{\lambda \in \Gamma_n} (x - \lambda) = \prod_{d|n} \prod_{\lambda \in \mathcal{R}_d} (x - \lambda) = \prod_{d|n} Q_d(x). \ \blacksquare$$

Remarque : ξ^j est une racine d-ième primitive de l'unité si et seulement si son ordre multiplicatif $\omega\left(\xi^j\right)$ vaut d. Comme

$$\omega\left(\xi^j\right) = \frac{\omega(\xi)}{\text{pgcd}(j,n)} = \frac{n}{\text{pgcd}(j,n)},$$

cela équivaut à dire que j appartient à $I_d = \left\{j \in [0..n-1] \ / \ \text{pgcd}(j,n) = \frac{n}{d}\right\}$. Ainsi

$$Q_d(x) = \prod_{j \in I_d} \left(x - \xi^j\right)$$

et $\{I_d\}_{d|n}$ forme une partition de $[0..n-1]$ (si n et m sont deux entiers tels que $n \leq m$, on note $[n..m] = \{n, ..., m\}$).

Corollaire 1 *Les polynômes cyclotomiques sur K sont unitaires. Ils appartiennent à $\mathbb{Z}[x]$ si $p = 0$, et à $\mathbb{F}_p[x]$ dans le cas contraire.*

Preuve : Par récurrence sur n. La propriété est triviale si $n = 1$ puisque $Q_1(x) = x - 1$. Si la propriété est vraie jusqu'au rang $n - 1$, la formule du Théorème 2 montre immédiatement que Q_n est unitaire. On peut écrire

$$x^n - 1 = f(x) Q_n(x) \quad \text{où } f(x) = \prod_{d|n \text{ et } d \neq n} Q_d(x).$$

L'hypothèse récurrente montre que le polynôme $f(x)$ appartient à $\mathbb{Z}[x]$ ou $\mathbb{F}_p[x]$ suivant le cas, et par conséquent l'unicité du quotient et du reste d'une division euclidienne de polynômes implique l'appartenance de $Q_n(x)$ à $\mathbb{Z}[x]$ ou à $\mathbb{F}_p[x]$. En effet, si nous nous plaçons par exemple dans le cas de la caractéristique nulle, la division euclidienne de $x^n - 1$ par $f(x)$ dans $\mathbb{Z}[x]$ (possible puisque $f(x)$ est unitaire) montre l'existence de deux polynômes $q(x)$ et $r(x)$ de $\mathbb{Z}[x]$ tels que $x^n - 1 = f(x) q(x) + r(x)$ et $\deg r(x) < \deg f$. Cette égalité polynomiale vraie dans $\mathbb{Z}[x]$ le sera à fortiori dans $\Sigma_n[x]$ où l'on a déjà $x^n - 1 = f(x) Q_n(x)$. L'unicité du quotient et du reste d'une division euclidienne dans $\Sigma_n[x]$ entraîne alors $Q_n(x) = q(x) \in \mathbb{Z}[x]$. ■

Corollaire 2 *$Q_n(x)$ divise tous les polynômes $\frac{x^n-1}{x^d-1}$ où d représente un diviseur de n distinct de n.*

Preuve : Les polynômes $Q_n(x)$ et $x^d - 1$ n'ayant pas de racine commune dans une clôture algébrique de K, seront premier entre eux. Il suffit alors de voir que $Q_n(x)$ divise le polynôme

$$x^n - 1 = \left(x^d - 1\right) \frac{x^n - 1}{x^d - 1}$$

et d'appliquer le Théorème de Gauss. ■

Corollaire 3 *Si r est un nombre premier, $Q_r(x) = x^{r-1} + x^{r-2} + ... + x + 1$.*

Preuve : En effet,

$$x^r - 1 = \prod_{d|r} Q_d(x) = (x - 1) Q_r(x). \blacksquare$$

Corollaire 4 *Si r est un nombre premier et $k \in \mathbb{N}^*$,*

$$Q_{r^k}(x) = x^{(r-1)r^{k-1}} + ... + x^{2r^{k-1}} + x^{r^{k-1}} + 1 = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}.$$

Preuve : En appliquant deux fois la formule du Théorème 2,

$$x^{r^k} - 1 = Q_{r^k}(x) \times \prod_{d|r^{k-1}} Q_d(x) = Q_{r^k}(x) \left(x^{r^{k-1}} - 1\right). \blacksquare$$

3 Calcul explicite de $Q_n(x)$

3.1 Par le Théorème 2

Théorème 3 *Soient $m, k \in \mathbb{N}$ et r un nombre premier.*
1) Si r ne divise pas m, $Q_{mr}(x).Q_m(x) = Q_m(x^r)$,
2) Si r divise m, $Q_{mr}(x) = Q_m(x^r)$,
3) Si r ne divise pas m,

$$Q_{mr^k}(x) = \frac{Q_m\left(x^{r^k}\right)}{Q_m\left(x^{r^{k-1}}\right)}.$$

Preuve : 1) Les polynômes des premiers et second membres ont même degré (en effet $\varphi(mr) + \varphi(m) = r\varphi(m)$ où φ représente la fonction d'Euler) et des racines simples. L'égalité sera donc assurée si l'on vérifie que toute racine de $Q_{mr}(x).Q_m(x)$ est aussi une racine de $Q_m(x^r)$. Ici :

$$\begin{aligned} \xi \text{ racine de } Q_{mr}(x) &\Leftrightarrow \xi \text{ racine primitive } (mr)\text{-ième de l'unité} \\ &\Rightarrow \xi^r \text{ racine primitive } m\text{-ième de l'unité} \\ &\Rightarrow \xi \text{ racine de } Q_m(x^r). \end{aligned}$$

$$\begin{aligned} \xi \text{ racine de } Q_m(x) &\Leftrightarrow \xi \text{ racine primitive } m\text{-ième de l'unité} \\ &\Rightarrow \xi^r \text{ racine primitive } m\text{-ième de l'unité (car } \operatorname{pgcd}(r,m) = 1) \\ &\Rightarrow \xi \text{ racine de } Q_m(x^r). \end{aligned}$$

2) On applique la même méthode qu'en 1). Les deux polynômes ont même degré, des racines simples, et $Q_{mr}(\xi) = 0$ entraîne $Q_m(\xi^r) = 0$.

3)

$$Q_{mr^k}(x) \underset{2)}{=} Q_{mr^{k-1}}(x^r) = \ldots \underset{2)}{=} Q_{mr}\left(x^{r^{k-1}}\right) \underset{1)}{=} \frac{Q_m\left(x^{r^k}\right)}{Q_m\left(x^{r^{k-1}}\right)}. \blacksquare$$

Exemple : La troisième formule du Théorème 3 permet de calculer explicitement n'importe quel polynôme cyclotomique. Par exemple

$$Q_{120}(x) = Q_{2^3.3.5}(x) = \frac{Q_{3.5}\left(x^{2^3}\right)}{Q_{3.5}\left(x^{2^{3-1}}\right)} = \frac{Q_{3.5}(x^8)}{Q_{3.5}(x^4)}$$

puis

$$Q_{3.5}(x) = \frac{Q_3(x^5)}{Q_3(x)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

entraînent

$$Q_{120}(x) = x^{32} + x^{28} - x^{20} - x^{16} - x^{12} + x^4 + 1.$$

3.2 Par la formule de Moebius

Définition 3 *La* ***fonction de Moebius*** *est la fonction arithmétique* $\mu : \mathbb{N}^* \to \mathbb{N}$ *définie par* $\mu(1) = 1$ *et*

$$\mu(n) = \begin{cases} 0 & \text{s'il existe un indice } i \text{ tel que } \alpha_i \geq 2, \\ (-1)^k & \text{sinon,} \end{cases}$$

où $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ *représente la décomposition en produits de facteurs premiers de* n *avec* $\alpha_i \geq 1$ *pour tout* i*.*

La fonction de Moebius permet d'inverser certaines relations sommatoires.

Théorème 4 ***Formule d'inversion de Moebius***
1) Version additive : Si $(G, +)$ *est un groupe additif, et si* f *et* g *sont des fonctions de* $\mathbb{N}$ *dans* G*,*

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} g(d) \, \mu\left(\frac{n}{d}\right).$$

2) Version multiplicative : Si $(G, .)$ *est un groupe multiplicatif, et si* f *et* g *sont des fonctions de* $\mathbb{N}$ *dans* G*,*

$$g(n) = \prod_{d|n} f(d) \Leftrightarrow f(n) = \prod_{d|n} g(d)^{\mu\left(\frac{n}{d}\right)}.$$

Corollaire 5 *On suppose* $\operatorname{pgcd}(n, q) = 1$*. Le polynôme cyclotomique d'indice* n *sur* $\mathbb{F}_q$ *est donné par*

$$Q_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu\left(\frac{n}{d}\right)}.$$

Preuve : On inverse la formule $x^n - 1 = \prod_{d|n} Q_d(x)$ grâce au Théorème de Moëbius et en se plaçant dans le groupe multiplicatif des fractions rationnelles $\mathbb{F}_q(x)$. ■

Exemple : Dans $\mathbb{F}_q$ et si $\operatorname{pgcd}(15, q) = 1$, on trouve

$$\begin{aligned} Q_{15}(x) &= \prod_{d|15} \left(x^d - 1\right)^{\mu\left(\frac{15}{d}\right)} \\ &= (x-1)^{\mu(15)} \left(x^3 - 1\right)^{\mu(5)} \left(x^5 - 1\right)^{\mu(3)} \left(x^{15} - 1\right)^{\mu(1)} \\ &= \frac{(x-1)\left(x^{15} - 1\right)}{(x^3 - 1)(x^5 - 1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1. \end{aligned}$$

4 Irréductibilité de $Q_n(x)$ dans $\mathbb{Q}[x]$

Nous allons prouver l'irréductibilité de Q_n sur $\mathbb{Q}[x]$ en utilisant la preuve de Landau (1929) que l'on peut trouver dans l'article d'Arnaudiès [1]. Cet article contient aussi une preuve directe de l'irréductibilité de $Q_r(x) = x^{r-1} + ... + x + 1$ lorsque r est premier dûe à Kronecker et n'utilisant pas le critère d'Eiseinstein.
La façon classique de montrer l'irréductibilité de Q_r consiste d'abord à vérifier que $Q_r(x)$ est irréductible sur $\mathbb{Z}[x]$ si et seulement si $Q_r(x+1)$ l'est, puis à écrire

$$Q_r(x+1) = \frac{(x+1)^r - 1}{x} = \sum_{k=1}^{r} \binom{r}{k} x^{k-1}$$

pour pouvoir appliquer le critère d'Eiseinstein. Cette preuve et celle du Théorème ci-dessous dépend du Lemme suivant :

Lemme 1 *Un polynôme primitif (resp. unitaire) P de $\mathbb{Z}[x]$ est irréductible dans $\mathbb{Q}[x]$ si et seulement si il est irréductible dans $\mathbb{Z}[x]$.*

Théorème 5 *Un polynôme cyclotomique sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$ et irréductible sur $\mathbb{Q}$.*

Preuve : On a déjà prouvé que $Q_n \in \mathbb{Z}[x]$ au Corollaire 1. Soit $P(x) = x^s + a_{s-1}x^{s-1} + ... + a_0$ un polynôme irréductible unitaire de $\mathbb{Z}[x]$ qui divise Q_n. Il en existe puisque $\mathbb{Z}[x]$ est un anneau factoriel et que Q_n est unitaire. Soit ξ une racine de P. Tout revient à prouver que $P(\xi^r) = 0$ pour tout nombre r premier avec n. Cela se fait en trois étapes.

a) Montrons que l'ensemble E des restes modulo P des polynômes $P\left(x^k\right)$, où $k \in \mathbb{N}$, est fini. Par division euclidienne

$$P\left(x^k\right) = P(x)\, Q_k(x) + R_k(x) \text{ avec } \deg R_k < s.$$

Si η est une racine de P, alors $P\left(\eta^k\right) = R_k(\eta)$. Par division euclidienne

$$\forall k \in \mathbb{N} \quad k = nq + k' \text{ avec } 0 \leq k' < n.$$

De $\eta^k = \eta^{k'}$ on déduit $R_k(\eta) = P\left(\eta^k\right) = P\left(\eta^{k'}\right) = R_{k'}(\eta)$. Les polynômes R_k et $R_{k'}$ coïncident en chacune des s racines distinctes de P. Etant de degré $< s$, ils seront égaux et E sera inclus dans $\{R_{k'}(\eta) \,/\, 0 \leq k' < n\}$.

b) Montrons l'assertion

$$\exists A \in \mathbb{N} \quad \forall p > A \quad p \text{ premier} \quad P(\xi) = 0 \Rightarrow P(\xi^p) = 0. \quad (*)$$

Comme E est fini, il existe un majorant A de toutes les valeurs absolues des coefficients des restes R de E. Soit p un nombre premier tel que $p > A$. On a

$$R_p(x) \equiv P(x^p) - (P(x))^p \quad (P).$$

Si $P(x) = \sum_i a_i x^i$, notons $\overline{P}(x) = \sum_i \dot{a}_i x^i$ le polynôme correspondant de $\mathbb{F}_p[x]$. Les égalités

$$\overline{P}(x^p) = \sum_i \dot{a}_i x^{pi} = \left(\sum_i \dot{a}_i x\right)^p = \left(\overline{P}(x)\right)^p$$

montrent que $P(x^p)-(P(x))^p \in p\mathbb{Z}[x]$. Comme $R_p(x)$ est le reste de la division euclidienne de $P(x^p)-(P(x))^p$ par le polynôme unitaire P, on déduit $R_p(x) \in p\mathbb{Z}[x]$. Mais $p > A$ et $R_p \in E$ entraînent $R_p = 0$, d'où $P(x^p) = P(x)Q_p(x)$. En substituant ξ à x on obtient $P(\xi^p) = 0$.

c) L'assertion $(*)$ se généralise par récurrence pour donner : Si $m = p_1^{\alpha_1}...p_k^{\alpha_k}$ où les entiers p_i sont premiers et $> A$, alors $P(\xi^m) = 0$.
Soit r premier avec n. Posons $m = r + n \prod_{p\in\mathcal{P}} p$ où $\mathcal{P}$ désigne tous les entiers naturels premiers p inférieurs ou égaux à A et ne divisant pas r. On a $\xi^r = \xi^m$ et m n'est divisible par aucun des entiers premiers p inférieurs strictement à A. D'après ce qui précède $P(\xi^r) = P(\xi^m) = 0$. ■

5 Le cas d'un corps fini

Un polynôme cyclotomique dans $\mathbb{F}_q[x]$ n'est pas nécessairement irréductible. Par exemple le polynôme $Q_{18}(x) = x^6 - x^3 + 1 \in \mathbb{F}_{17}[x]$ se décompose en

$$Q_{18}(x) = \left(x^2 + 7x + 1\right)\left(x^4 - 7x^3 + 14x^2 - 7x + 1\right).$$

Le Théorème suivant précise la décomposition de $Q_n(x)$ en produit de facteurs iréductibles.

Théorème 6 *Supposons que* $\text{pgcd}(n,p) = 1$ *et appelons* $m = \omega_n(q)$ *l'ordre multiplicatif de* q *modulo* n *(i.e. le plus petit entier strictement positif* d *tel que* $q^d \equiv 1 \ (n)$*).*
1) Le n*-ième corps cyclotomique* Σ_n *sur* $\mathbb{F}_q$ *est une extension algébrique simple de* $\mathbb{F}_q$*. On a* $\Sigma_n = \mathbb{F}_{q^m} = \mathbb{F}_q(\xi)$ *pour toute racine primitive* n*-ième de l'unité* ξ*.*
2) Le polynôme cyclotomique $Q_n(x)$ *s'écrit comme le produit de* $\frac{\varphi(n)}{m}$ *polynômes irréductibles distincts de degrés* m*, et* Σ_n *est le corps de décomposition de l'un quelconque de ces polynômes.*

Preuve : 1) $\Sigma_n = \mathbb{F}_q(\xi)$ pour toute racine primitive n-ième de l'unité ξ. L'élément ξ est une racine primitive n-ième de l'unité si et seulement si c'est un élément d'ordre multiplicatif n dans la clôture algébrique de $\mathbb{F}_q$. Par suite

$$\xi \in \mathbb{F}_{q^t} \Leftrightarrow \xi^{q^t} = \xi \Leftrightarrow \xi^{q^t-1} = 1 \Leftrightarrow n | \left(q^t - 1\right)$$

et cela montre que $\mathbb{F}_{q^m}$ est le plus petit corps contenant $\mathbb{F}_q$ et ξ.
2) L'égalité $\mathbb{F}_q(\xi) = \mathbb{F}_{q^m}$ montre que le polynôme minimal de ξ est de degré m. Comme les racines de $Q_n(x)$ sont les racines primitives n-ièmes de l'unité, les seuls polynômes irréductibles intervenant dans la décomposition de $Q_n(x)$ seront ces polynômes minimaux. Ces polynômes minimaux seront distincts deux à deux puisque toutes les racines de $x^n - 1$ sont simples. ■

Théorème 7 $\mathbb{F}_q$ *est le* $(q-1)$*-ième corps cyclotomique de n'importe lequel de ses sous-corps.*

Preuve : Soit $\mathbb{F}_t \subset \mathbb{F}_q$ et ξ une racine primitive $(q-1)$-ième de l'unité. On a $\xi \in \mathbb{F}_q$ donc $\mathbb{F}_t(\xi) \subset \mathbb{F}_q$, et l'égalité $\mathbb{F}_q^* = \left\{1, \xi, ..., \xi^{q-2}\right\}$ prouve l'inclusion inverse. ■

6 Théorème de Wedderburn

Théorème 8 *Tout corps fini est commutatif.*

Preuve : Soient K un corps fini, $Z(K)$ son centre, et $q = \#Z(K)$. On a la tour de corps

$$Z(K) \subset N_a \subset K$$

où $N_a = \{x \in K \,/\, ax = xa\}$ est le normalisateur de a. L'ensemble K apparaît comme un $Z(K)$-espace vectoriel et un N_a-espace vectoriel à gauche. N_a est aussi un $Z(K)$-espace vectoriel. Posons

$$n = [K : Z(K)], \; e_a = [K : N_a] \text{ et } d_a = [N_a : Z(K)].$$

On a clairement $n = e_a d_a$, $\#N_a = q^{d_a}$ et $\#K = q^n$. Le groupe $G = K^*$ opère sur lui-même par conjugaison. L'équation des classes s'écrit :

$$\#K^* = \#Z(K^*) + \sum_x \#G_x \quad (*)$$

où $G_x = \left\{y \in K^* \,/\, \exists g \in K^* \quad y = gxg^{-1}\right\}$ est l'orbite de x. On sait que $G_x \simeq G/H_x$ où H_x est le stabilisateur de x (encore appelé le sous-groupe d'isotropie de x). Ici

$$H_x = \left\{g \in K^* \,/\, gxg^{-1} = x\right\} = \{g \in K^* \,/\, gx = xg\} = N_x^*.$$

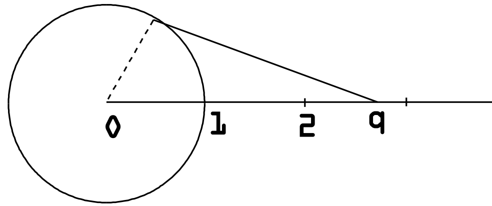
Donc

$$\#G_x = \frac{\#K^*}{\#N_x^*} = \frac{q^n - 1}{q^{d_x} - 1}.$$

La somme $(*)$ porte sur les $x \in K^*$ qui représentent des orbites distinctes. Comme d_x divise n, si m_d désigne le nombre de termes de la somme tels que $\#N_x = q^d$, la formule $(*)$ devient

$$q^n - 1 = q - 1 + \sum_{d \in \mathcal{D}} m_d \frac{q^n - 1}{q^d - 1} \quad (\clubsuit)$$

où $\mathcal{D}$ est un sous-ensemble de l'ensemble des diviseurs de n (éventuellement vide).
$n \notin \mathcal{D}$ sinon il existerait $x \in K^*$ tel que $\#N_x^* = \#K^*$, i.e. $N_x^* = K^*$. Cela équivaut à $x \in Z(K^*)$ et dans ce cas, x a déjà été compté dans $\#Z(K^*)$.
Pour démontrer le Théorème, il faut prouver que $n = 1$. On raisonne par l'absurde : si $n > 1$ et si $d \in \mathcal{D}$, alors $d|n$, $d \neq n$ et le Corollaire 2 montre que $Q_n(x)$ divise $\frac{x^n-1}{x^d-1}$, donc $Q_n(q)$ divise $\frac{q^n-1}{q^d-1}$. La formule $(\clubsuit)$ montre alors que $Q_n(q)$ divise $q - 1$.



On a $Q_n(q) = \prod_{\text{pgcd}(i,n)=1} (q - \xi^i)$. Si i est premier avec n, on sait que ξ^i est sur le cercle trigonométrique et n'est pas égal à 1. Comme $q \geq 2$ (en effetm K contient au moins 0 et 1), on déduit

$$\left|q - \xi^i\right| > |q| - \left|\xi^i\right| = q - 1$$

d'où $|Q_n(q)| > q - 1$ et la contradiction. ■

References

[1] Arnaudiès, L'irréductibilité des polynômes cyclotomiques, RMS 91-92, p. 145.

[2] R. Lidl & H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, vol. **20**, Addison-Weysley Publishing Company, 1983.

[3] J. Querré, Cours d'Algèbre, Maîtrise de Mathématiques, Masson, 1976.